Funzione di sicurezza: Barriera fotoelettrica
Prodotti: barriera fotoelettrica
controllore GuardLogix®

Livello di sicurezza: PLe, Cat. 4 in conformità ad
EN ISO 13849.1 2008

Indice

Introduzione

Nella presente nota applicativa, dedicata alle funzioni di sicurezza, sono illustrate le procedure di cablaggio, configurazione e programmazione di un controllore Compact GuardLogix® e di un modulo POINT Guard I/O™ per il monitoraggio di una barriera fotoelettrica GuardShield 440L. In caso di richiesta di intervento della barriera fotoelettrica, o di rilevamento di un guasto nel circuito di monitoraggio, il controllore GuardLogix diseccita il dispositivo di controllo finale, che in questo caso è rappresentato da una coppia di contattori 100S ridondanti.

In questo esempio si farà riferimento ad un controllore Compact GuardLogix, ma le descrizioni qui riportate valgono per qualsiasi controllore GuardLogix. In questo esempio si fa riferimento ad una barriera fotoelettrica GuardShield 440L, ma le descrizioni qui riportate valgono per tutte le barriere fotoelettriche che eseguono prove ad impulsi sulle uscite OSSD1 ed OSSD2. I calcoli di SISTEMA riportati più avanti in questo documento dovrebbero essere rieseguiti con i prodotti effettivamente utilizzati.

Informazioni importanti per l'utente

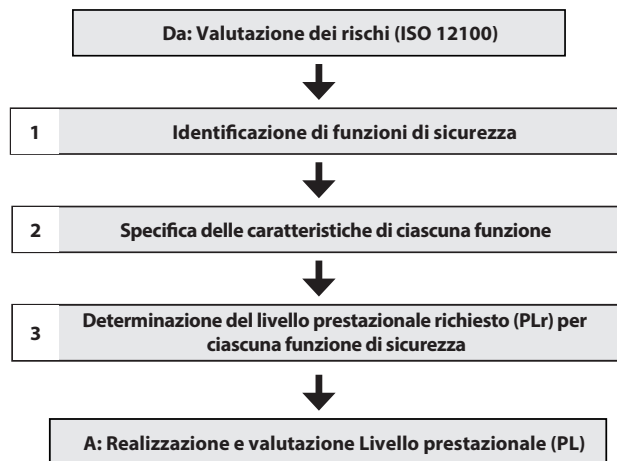
Le apparecchiature a stato solido hanno caratteristiche di funzionamento differenti rispetto a quelle elettromeccaniche. Il documento Safety Guidelines for the Application, Installation and Maintenance of Solid State Controls (pubblicazione **SGI-1.1** disponibile presso l'Ufficio Commerciale Rockwell Automation di zona oppure online all'indirizzo **http://www.rockwellautomation.com/literature/**) descrive alcune importanti differenze tra le apparecchiature a stato solido ed i dispositivi elettromeccanici cablati. A causa di tali differenze e dell'ampia gamma di utilizzi delle apparecchiature a stato solido, tutto il personale responsabile dell'applicazione dell'apparecchiatura deve verificare che vengano soddisfatti i criteri di corretto utilizzo dell'apparecchiatura.

In nessun caso Rockwell Automation, Inc. sarà responsabile per danni indiretti o consequenziali derivanti dall'utilizzo o dall'applicazione di questa apparecchiatura.

Gli esempi e gli schemi contenuti nel presente manuale sono inclusi solo a scopo illustrativo. A causa delle numerose variabili e dei diversi requisiti relativi ad una particolare installazione, Rockwell Automation, Inc. non può essere ritenuta responsabile per l'utilizzo effettivo basato sugli esempi e sugli schemi qui riportati.

Rockwell Automation, Inc. non si assume alcuna responsabilità di brevetto per quanto riguarda l'utilizzo di informazioni, circuiti elettrici, apparecchiature o software descritti nel presente manuale.

Realizzazione delle funzioni di sicurezza: valutazione dei rischi

Per conoscere il livello prestazionale richiesto occorre eseguire una valutazione dei rischi, al fine di determinare l'entità della riduzione dei rischi che deve essere garantita dai componenti di sicurezza del sistema di controllo. Nell'ambito del processo di riduzione dei rischi occorre anche determinare le funzioni di sicurezza della macchina. Per le finalità previste da questo documento, si presuppone che il livello prestazionale richiesto sia Categoria 4, PLe.

Funzione di sicurezza di arresto di emergenza

Arresto di emergenza tramite attivazione di una barriera fotoelettrica; POC (Point of Operation Control). In questo esempio non è prevista una funzione di muting.

Requisiti delle funzioni di sicurezza

L'interruzione della barriera fotoelettrica determina un arresto del moto pericoloso, che viene evitato tramite disattivazione dell'alimentazione al motore. Al ripristino della barriera fotoelettrica, il moto pericoloso e l'alimentazione del motore non sono ripristinati fino a quando non viene eseguita un'azione secondaria (pressione del pulsante di avviamento). I guasti relativi alla barriera fotoelettrica, i morsetti di cablaggio o il controllore di sicurezza saranno rilevati prima della successiva richiesta di intervento di sicurezza. La distanza di sicurezza della barriera fotoelettrica deve essere determinata in modo che il moto pericoloso possa essere arrestato prima che l'utente possa raggiungere il pericolo. La funzione di sicurezza descritta in questo esempio è in grado di attivare e disattivare l'alimentazione dei motori con valori nominali fino a 9 A, 600 V CA.

La funzione di sicurezza sarà conforme ai requisiti previsti per la Categoria 4, Livello prestazionale "e" (Cat 4, PLe), in conformità alla norma ISO 13849-1, e SIL3 in conformità alla norma IEC 62061, e garantirà un funzionamento affidabile in conformità alla norma ANSI B11.19.

Le note riportate in questo manuale hanno lo scopo di evidenziare le considerazioni in materia di sicurezza.

	Avvertenza: Identifica le informazioni sulla prassi o sulle circostanze che possono causare un'esplosione in un'area pericolosa che potrebbero comportare lesioni personali o morte, danni alle cose o perdite economiche.
IMPORTANTE	Identifica le informazioni indispensabili per una corretta applicazione e per la comprensione del prodotto.
	Attenzione: Identifica informazioni su procedure o circostanze che possono causare lesioni personali o morte, nonché danni materiali o economici. I segnali di attenzione aiutano ad individuare i pericoli, ad evitarli ed a riconoscerne le conseguenze.
	Pericolo di folgorazione: Le etichette possono essere apposte sopra o all'interno dell'apparecchiatura (ad esempio, convertitore di frequenza o motore) per avvertire della possibile presenza di tensione pericolosa.
	Pericolo di ustioni: Le etichette possono essere apposte sopra o all'interno dell'apparecchiatura (ad esempio, convertitore di frequenza o motore) per avvertire che le superfici possono raggiungere temperature pericolose.

Informazioni generali sulla sicurezza

Gli utenti sono invitati a contattarci per richiedere ulteriori informazioni sui nostri servizi di valutazione dei rischi per la sicurezza.

IMPORTANTE	Questo esempio applicativo è destinato ad utenti di livello avanzato, che si presuppone abbiano ricevuto una formazione specifica e siano esperti in materia di requisiti dei sistemi di sicurezza.
	Attenzione: è necessario eseguire una valutazione dei rischi per sincerarsi di aver individuato ed affrontato tutte le combinazioni di attività e rischi. In seguito alla valutazione dei rischi, potrebbe essere necessario aggiungere dei circuiti per ridurre il rischio portandolo ad un livello accettabile. Per la progettazione dei circuiti di sicurezza sono necessari calcoli delle distanze di sicurezza non presi in considerazione nell'ambito di questo documento.

Descrizione del concetto di sicurezza funzionale

Il moto pericoloso viene interrotto o impedito tramite interruzione della barriera fotoelettrica. La barriera fotoelettrica (LC1) è collegata ad una coppia di ingressi di sicurezza sul modulo d'ingresso di sicurezza (SI1). I contattori di sicurezza (K1 e K2) sono collegati ad una coppia di uscite di sicurezza su un modulo d'uscita di sicurezza (SO1). Il modulo I/O è connesso al controllore di sicurezza (SC1) tramite CIP Safety su rete EtherNet/IP. Il codice di sicurezza di SC1 monitora lo stato della barriera fotoelettrica tramite l'istruzione di sicurezza precertificata DCS (Dual Channel Input Stop). Quando le condizioni previste per tutti gli interblocchi di ingresso di sicurezza sono soddisfatte, non sono rilevati guasti, e viene premuto il pulsante di reset, un secondo blocco funzione certificato denominato CROUT (Configurable Redundant Output) controlla e monitora il feedback per una coppia di contattori 100S ridondanti. Riepilogando, quando la barriera fotoelettrica viene bloccata, i contattori vengono diseccitati. Quando la barriera fotoelettrica viene sbloccata e si preme il pulsante di reset, i contattori vengono eccitati.

Elenco dei componenti

In questo esempio applicativo sono utilizzati i componenti elencati di seguito.

Numero di catalogo	Descrizione	Quantità
440L-P4JL0640YD	Barriera fotoelettrica di sicurezza GuardShield™, risoluzione 14 mm, altezza del campo di protezione 640 mm, 64 raggi, allineamento laser integrato	1
889D-F4AC-2	Micro CC (M12), femmina, diritto, 4 pin, cavo in PVC, giallo, non schermato, sezione 0,32 mm² (22 AWG), 2 metri	1
889D-F8AB-2	Micro CC (M12), femmina, diritto, 8 pin, cavo in PVC, giallo, non schermato, sezione 0,20 mm² (24 AWG), 2 metri	1
800FM-G611MX10	Pulsante di reset 800F – Metallo, con protezione, blu, R, portacontatti in metallo, 1 contatto N.A, standard	1
100S-C09ZJ23C	Serie 100S-C – Contattori di sicurezza	2
1768-ENBT	Modulo bridge EtherNet/IP CompactLogix™	1
1768-L43S	Processore Compact GuardLogix©, memoria standard 2,0 MB, memoria di sicurezza 0,5 MB	1
1768-PA3	Alimentatore, ingresso 120/240 V CA, 3,5 A a 24 V CC	1
1769-ECR	Terminazione destra	1
1734-AENT	Scheda Ethernet 24 V CC	1
1734-TB	Base modulo con morsetti a vite IEC rimovibili	4
1734-IB8S	Modulo d'ingresso di sicurezza POINT Guard	1
1734-OB8S	Modulo d'uscita di sicurezza POINT Guard	1
1783-US05T	Switch Ethernet non gestito Stratix 2000™	1

Configurazione e cablaggio

Per informazioni dettagliate sull'installazione ed il cablaggio, consultare i manuali dei prodotti, elencati nella sezione Altre risorse.

Cenni generali sul sistema

Il modulo d'ingresso 1734-IB8S monitora le uscite OSSD1 ed OSSD2 dalla barriera fotoelettrica 440L. Se la barriera fotoelettrica viene bloccata, le uscite OSSD1 ed OSSD2 passano a LO, ed il controllore reagisce diseccitando i contattori di sicurezza.

La barriera 440L è dotata di funzioni diagnostiche integrate che consentono di testare dinamicamente il cablaggio di segnale per rilevare eventuali cortocircuiti a 24 V CC e cortocircuiti tra canali. Se si verifica un guasto, l'uscita OSSD1 o OSSD2 o entrambe vengono impostate su LO, ed il controllore reagisce diseccitando i contattori di sicurezza.

I cortocircuiti a 0 VCC (e la mancanza di un conduttore) vengono interpretati come un circuito aperto dal modulo d'ingresso 1734-IB8S ed il controllore reagisce diseccitando i contattori di sicurezza. Se la discrepanza tra gli ingressi si protrae per un tempo superiore al tempo di discrepanza previsto, il blocco funzione (DCS) nel controllore segnalerà un guasto. Il blocco funzione viene ripristinato solo in seguito all'eliminazione del guasto e ad un ciclo di blocco/sblocco della barriera fotoelettrica.

Il dispositivo di controllo finale in questo caso è costituito da una coppia di contattori di sicurezza 100S, K1 e K2. I contattori sono controllati da un modulo d'uscita di sicurezza 1734-OBS. I contattori sono collegati in una configurazione in serie ridondante. Vi è inoltre un circuito di feedback collegato attraverso i contatti NA, con ritorno ad un ingresso sul modulo 1734-IB8S per monitorare i contattori garantendo un funzionamento corretto. I contattori non possono essere riavviati se il circuito di feedback non è nello stato corretto.

Il sistema è provvisto di pulsanti di ripristino individuali per il reset degli errori/guasti e delle uscite di sicurezza.

Si noti che in questo esempio i pulsanti di reset e il circuito di feedback del contattore sono tutti collegati al modulo 1734-IB8S, ma ciò non è necessario dal punto di vista della sicurezza funzionale. Questi tre (3) ingressi potrebbero anche essere collegati ad un modulo d'ingresso standard.

Calcolo della distanza di sicurezza

L'utente dovrà eseguire un calcolo per determinare la distanza tra la barriera fotoelettrica ed il pericolo, applicando la seguente formula. Nella pratica si dovranno usare i valori specifici dell'applicazione anziché i calcoli di esempio riportati di seguito.

S = (K * T) + C

K = 63 pollici al secondo (costante riportata nello standard ANSI B11.19-1990)

T = tempo di arresto

C = fattore di penetrazione in profondità = 1 pollice (per una risoluzione di 14 mm; ricavato dalla documentazione)

Il tempo di arresto (T) in questo esempio è dato dalla somma dei seguenti valori:

a) ritardo della barriera fotoelettrica = 25 ms (ricavato dalla documentazione)
b) ritardo del modulo 1734-IB8S = 16 ms (ricavato dalla documentazione)
c) ritardo della connessione del modulo d'ingresso
d) ritardo del controllore di sicurezza
   Watchdog del task di sicurezza
   Periodo del task di sicurezza
e) ritardo della connessione del modulo d'uscita
f) ritardo di 1734-OB8S = 6 ms (ricavato dalla documentazione)
g) tempo di risposta del contattore = 15 ms (ricavato dalla documentazione)
h) tempo di arresto effettivo della macchina = ai fini di questo esempio si suppone pari a 900 ms

C – il ritardo di default della connessione del modulo d'ingresso è pari a 4 x RPI

Supponendo che RPI sia pari a 10 ms, il ritardo massimo sarà di 40 ms

E – il ritardo di default della connessione del modulo d'uscita è pari a 3 x RPI

Supponendo che RPI sia pari a 10 ms, il ritardo massimo sarà di 30 ms

Il tempo di reazione del caso peggiore può essere calcolato supponendo che si verifichi un guasto singolo nel sistema di controllo. In tal caso nel calcolo del tempo si dovrà considerare solo il valore più alto tra i due ritardi delle connessioni sopra indicati. In questo esempio si utilizzerà il valore di 40 ms, mentre il valore 30 viene escluso. Se si vuole anche tenere conto del caso in cui si verificano più guasti contemporaneamente, utilizzare entrambi i valori nel calcolo.

D – il ritardo del controllore di sicurezza è dato dalla combinazione del periodo del task di sicurezza più il watchdog del task di sicurezza. Il watchdog serve a tenere conto della possibilità che il codice di sicurezza venga eseguito fino al watchdog, ma non ne determini l'intervento. Il periodo del task di sicurezza serve a tenere conto della possibilità che la scansione asincrona si concluda esattamente quando l'ingresso cambia stato. Ai fini di questo esempio, si presuppone quanto segue:

Periodo del task di sicurezza = 10 ms

Watchdog del task di sicurezza = 5 ms

Quindi, per calcolare T, sommare i seguenti valori:

Ritardo della barriera fotoelettrica = 25 ms

Ritardo del modulo 1734-IB8S = 16 ms

Ritardo maggiore della connessione del modulo d'ingresso/uscita = 40 ms

Ritardo del controllore di sicurezza = 10 + 5 = 15 ms

Ritardo di 1734-OB8S = 6 ms

Tempo di risposta del contattore = 15 ms

Tempo di arresto effettivo della macchina = 900 ms

Il tempo di arresto totale risulta quindi essere (T) = 1017 ms

S = (K * T) + C = (63 * 1,017) + 1 = 65,071 pollici (1,65 metri)

In base a questo esempio, la barriera fotoelettrica deve quindi essere collocata a 1,65 m di distanza dal pericolo.

Calcolo della distanza di sicurezza secondo 13855

S = (K x T) + C
S: distanza minima in millimetri (mm)

K: parametro in millimetri al secondo (mm/s), ricavato dai dati sulla velocità d'avvicinamento del corpo o di parti del corpo

T: tempo di arresto totale in secondi

C: distanza di intrusione in mm

Nella presente nota applicativa vengono adottati i seguenti valori:

K = 1600 mm/secondo
T = Somma di

Ritardo della barriera fotoelettrica = 25 ms

Ritardo del modulo 1734-IB8S = 16 ms

Ritardo maggiore della connessione del modulo d'ingresso/uscita = 40 ms

Ritardo del controllore di sicurezza = 10 + 5 = 15 ms

Ritardo di 1734-OB8S = 6 ms

Tempo di risposta del contattore = 15 ms

Tempo di arresto effettivo della macchina = 900 ms

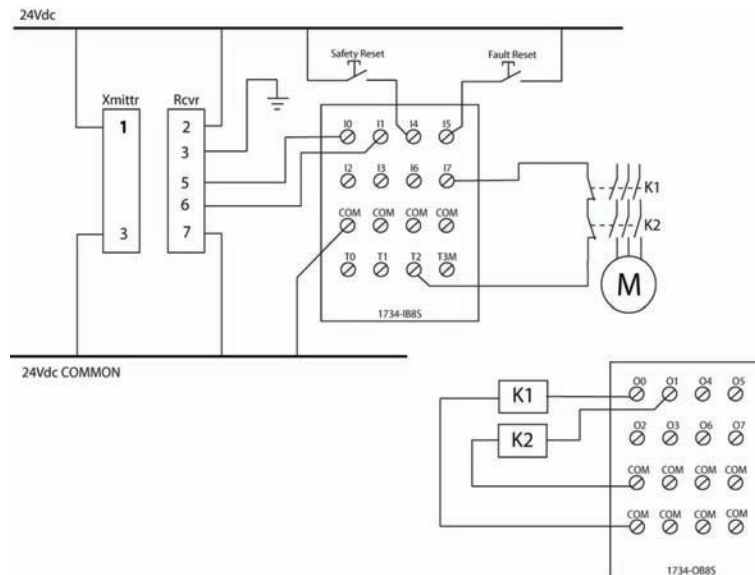
Il tempo di arresto totale risulta quindi essere (T) = 1017 ms

C = 8(d-14), ma non inferiore a 0, dove d è la risoluzione della barriera fotoelettrica

S = 1600 x 1,017 + 8(14 -14)

La barriera fotoelettrica non deve essere montata a una distanza inferiore a 1628 mm

dal moto pericoloso da cui si intende proteggersi.

Schemi elettrici

Configurazione

La barriera fotoelettrica 400L è provvista di microinterruttori che possono rimanere nella posizione predefinita in fabbrica.

Ricevitore – Impostazioni di fabbrica

Interruttore	Funzione dell'interruttore	Impostazione predefinita	Descrizione
1	Attivazione di modalità – La combinazione determina l'attivazione di una delle seguenti modalità: Solo protezione, Interblocco di avviamento, Interblocco di riavviamento	ON	Solo protezione
2		ON	
3	MPCE: Disabilitazione monitoraggio	ON	Disabilitato
4	Attivazione blanking fisso	OFF	Disabilitato
5	Attivazione blanking flottante – raggio singolo	OFF	Gli interruttori 5 e 6 non possono essere attivati ("On") contemporaneamente
6	Attivazione blanking flottante – due raggi	OFF	
7	Impostazione codifica raggio	OFF	Disabilitato
8	Non utilizzato	OFF	

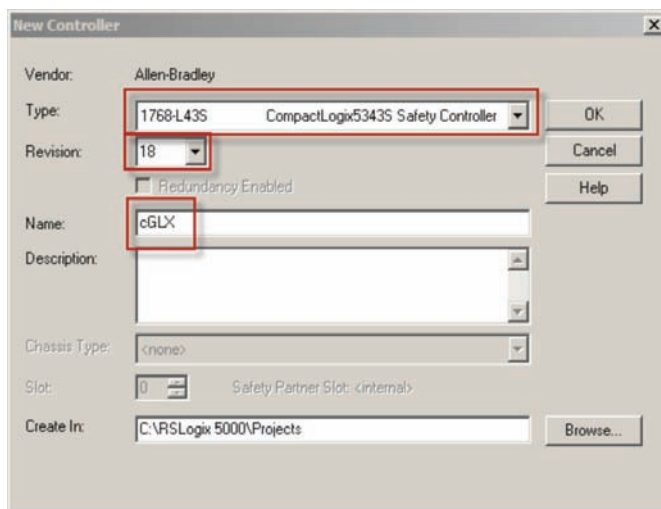
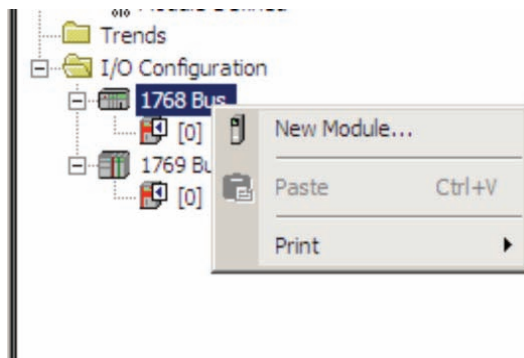
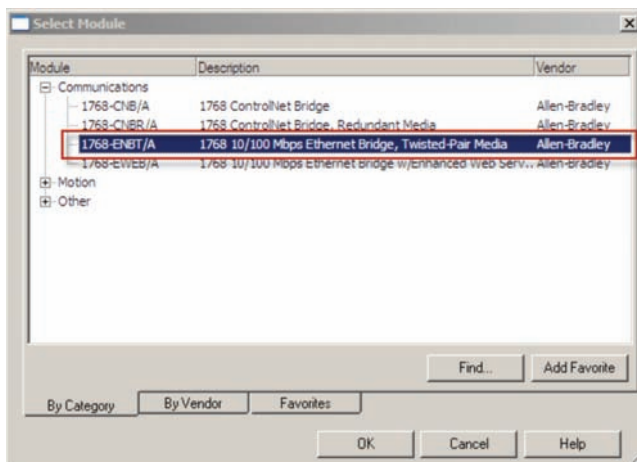
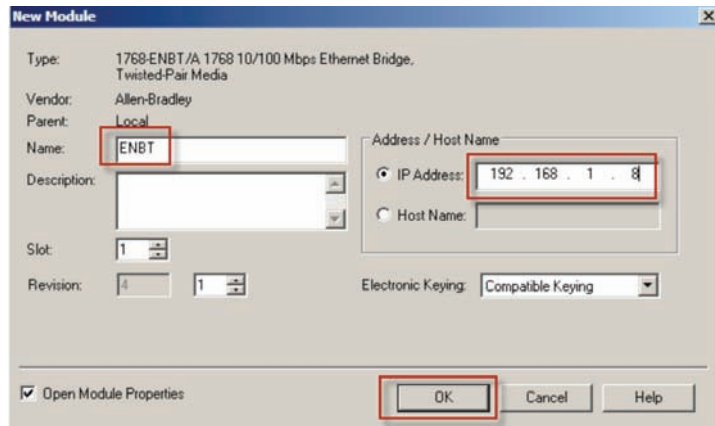
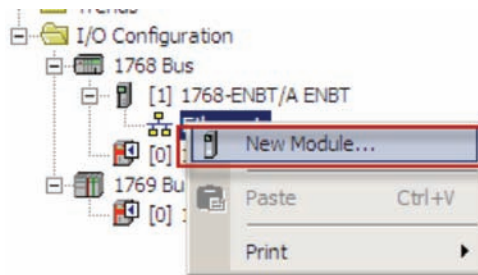
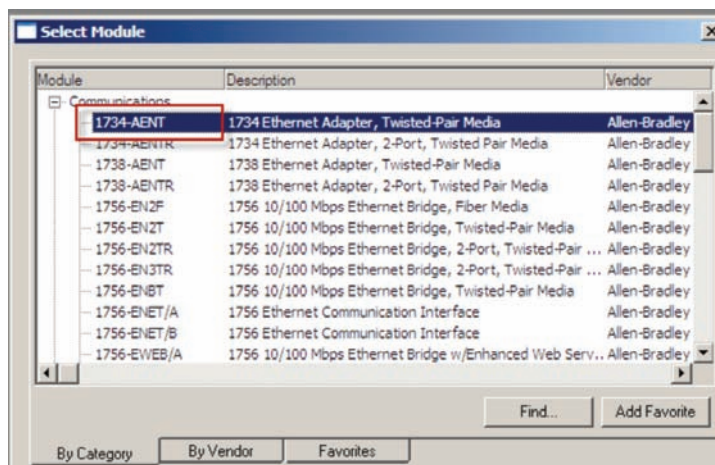
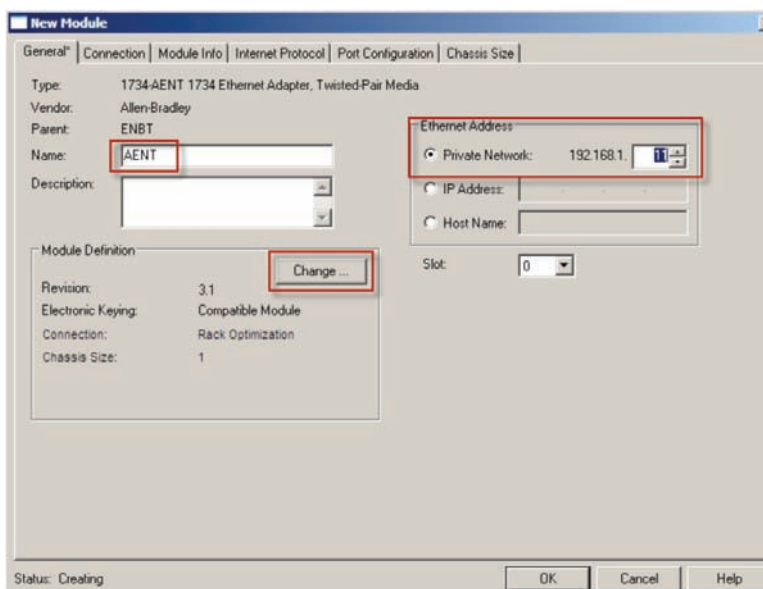
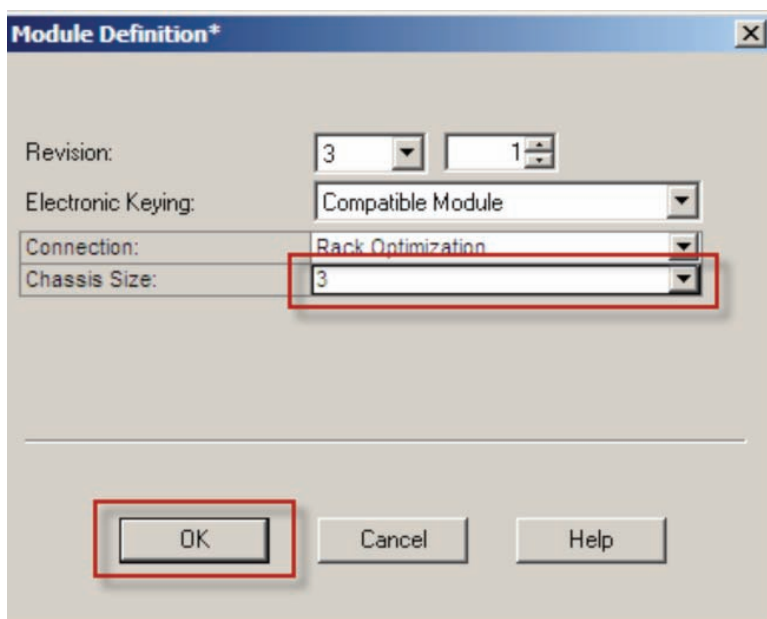
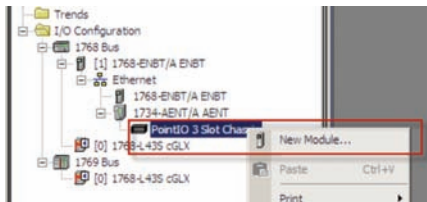
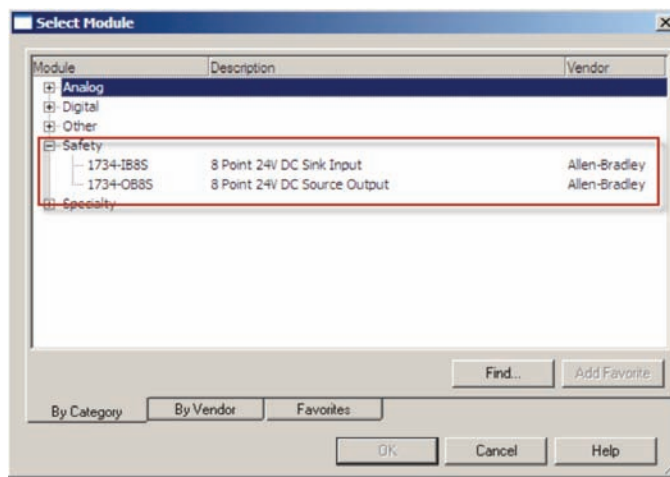
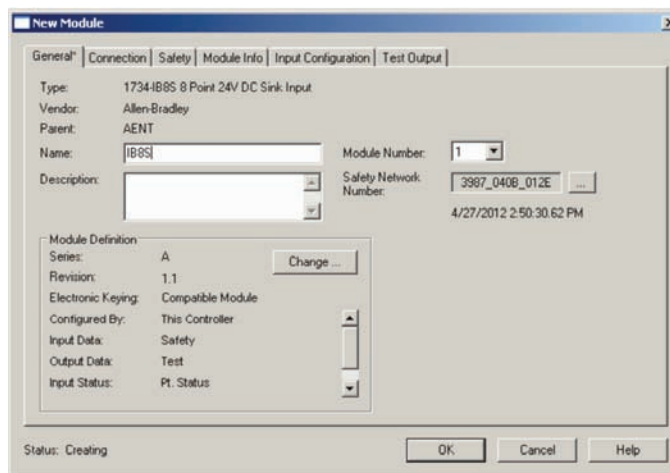
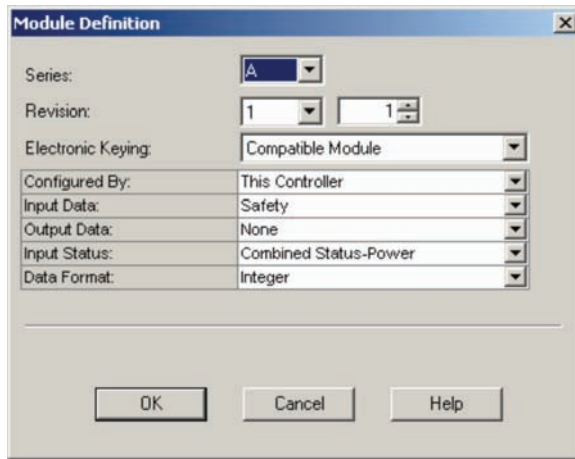
Trasmettitore – Impostazioni di fabbrica

Interruttore	Funzione dell'interruttore	Impostazione predefinita	Descrizione
1	Impostazione codifica raggio	OFF	Disabilitato
2	Segnale di prova macchina	OFF	OFF: Segnale High attivo – nessuna connessione o connessione normalmente aperta ON: Segnale Low attivo – connessione NC

Per la configurazione del controllore Compact GuardLogix si utilizza il software RSLogix™ 5000 versione 17 o successiva. Occorre creare un nuovo progetto ed aggiungere i moduli I/O, dopodiché si configurano i moduli I/O in base ai tipi di ingressi ed uscite corretti. In questo documento non è possibile fornire una descrizione dettagliata di tutte le fasi. La descrizione presuppone una conoscenza di base dell'ambiente di programmazione RSLogix.

Configurazione del controllore e dei moduli I/O aggiuntivi

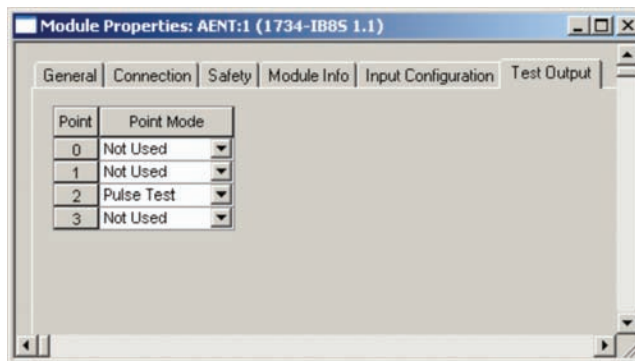
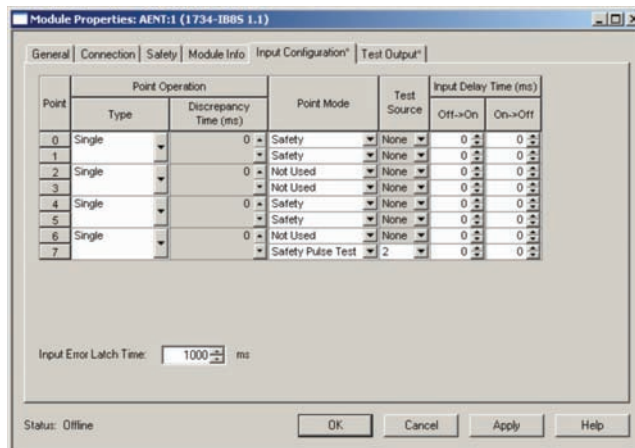
Attenersi alla seguente procedura.

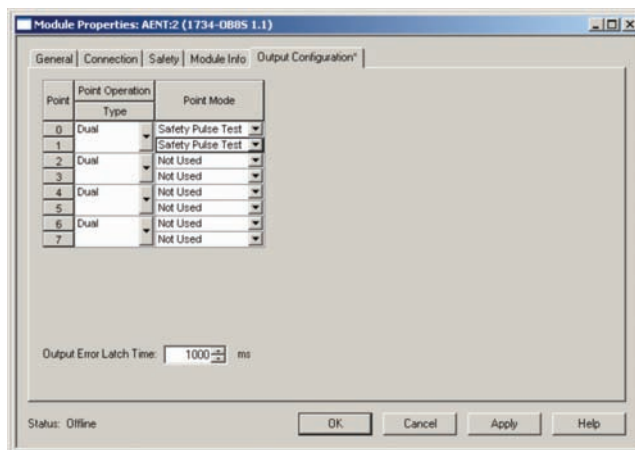
1. Nel software RSLogix 5000, creare un nuovo progetto.

2. Nell'Organizer del controllore, aggiungere il modulo 1768-ENBT alla sbarra 1768.

3. Selezionare il modulo 1768-ENBT e fare clic su OK.

4. Denominare il modulo, digitare il relativo indirizzo IP, quindi fare clic su OK. In questo esempio è stato utilizzato l'indirizzo 192.168.1.8. L'indirizzo dell'utente può essere diverso.

5. Aggiungere la scheda 1734-AENT facendo clic con il pulsante destro del mouse sul modulo 1768-ENBT nell'Organizer del controllore e selezionare New Module.

6. Selezionare la scheda 1734-ENBT e fare clic su OK.

7. Denominare il modulo, digitare il relativo indirizzo IP, quindi fare clic su OK. In questo esempio è stato utilizzato l'indirizzo 192.168.1.11. L'indirizzo dell'utente può essere diverso.
8. Fare clic su Change.

9. Impostare la dimensione dello chassis 3 (in Chassis Size) per la scheda 1734-AENT e fare clic su OK. La dimensione dello chassis è data dal numero di moduli che vi verranno inseriti. Si suppone che il modulo 1734-AENT si trovi nello slot 0, pertanto, nel caso di un modulo di ingresso ed un modulo di uscita, la dimensione dello chassis è pari a 3.

10. Nell'Organizer del controllore, fare clic con il pulsante destro del mouse sulla scheda 1734-AENT e scegliere New Module.

11. Espandere Safety, selezionare il modulo 1734-IB8S, quindi fare clic su OK.

12. Nella finestra di dialogo New Module, denominare il dispositivo "IB8S", quindi fare clic su Change.

13. Quando si aprirà la finestra di dialogo Module Definition, impostare Output Data su None e verificare che Input Status sia Combined Status-Power, quindi fare clic su OK. Impostare Output Data su "None" significa che non è possibile utilizzare le uscite di test come uscite standard: ciò non verrà fatto in questo esempio. Si noti che questo determina il salvataggio di una (1) connessione del controllore, poiché utilizzeremo solo la connessione di ingresso.

14. Chiudere la finestra di dialogo Module Properties facendo clic su OK.

15. Ripetere i passi da 10 a 14 per aggiungere il modulo d'uscita di sicurezza 1734-OB8S. Denominare il modulo OB8S. Si noti che tale modulo sarà nello slot 2; selezionare Combined Status-Readback-Power per la definizione di Input Status.

Configurazione dei moduli I/O

Per configurare i moduli POINT Guard I/O, attenersi alla seguente procedura.

1. Nell'Organizer del controllore, fare clic con il pulsante destro del mouse sul modulo 1734-IB8S e scegliere Properties.
2. Fare clic su Test Output e configurare il modulo come indicato in figura.

3. Fare clic su Input Configuration e configurare il modulo come indicato in figura. Gli ingressi 0/1 corrispondono alla barriera fotoelettrica. Gli ingressi 4/5 corrispondono ai pulsanti di reset. L'ingresso 7 corrisponde al circuito di monitoraggio dei contattori. Tenere presente che l'ingresso 7 è alimentato dall'uscita di test 2. Si noti che non vi è differenza tra la configurazione di sicurezza o standard di un canale d'ingresso. Questa distinzione è utile principalmente a scopo di documentazione.

4. Fare clic su OK.
5. Nell'Organizer del controllore, fare clic con il pulsante destro del mouse sul modulo 1734-OB8S e scegliere Properties.

6. Fare clic su Output Configuration e configurare il modulo come indicato in figura. La bobina elettromeccanica del contattore può essere sottoposta a prova ad impulsi senza reagire al breve impulso LO.

7. Fare clic su OK.

Programmazione

L'istruzione DCS (Dual Channel Input Stop) monitora i dispositivi di sicurezza a doppio ingresso, la cui funzione principale è quella di arrestare una macchina in sicurezza. Ad esempio, rientrano in questa categoria gli arresti di emergenza, le barriere fotoelettriche o gli interblocchi di sicurezza. In questo esempio viene utilizzata per monitorare una barriera fotoelettrica.

L'istruzione DCS verifica la coerenza dei canali a doppio ingresso (Equivalent – Active High) e rileva i guasti ed interviene in caso di rilevamento di un'incoerenza per un tempo superiore al tempo di discrepanza configurato (Discrepancy Time – ms).

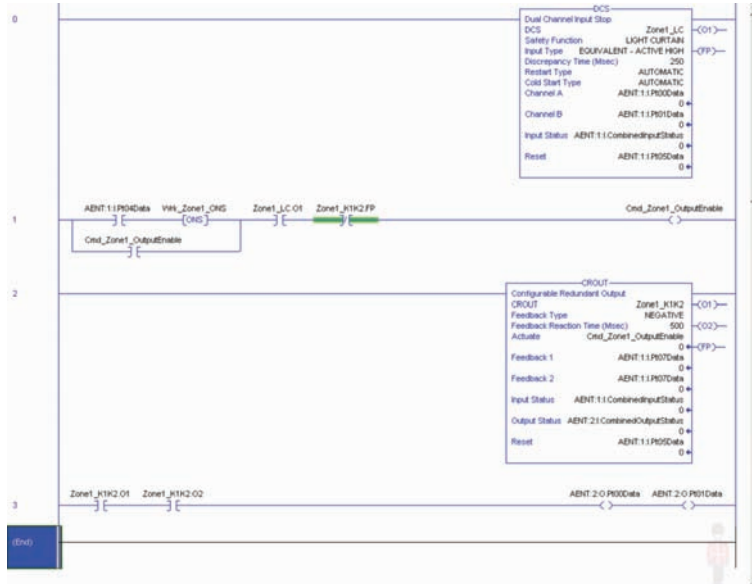
Il tipo di riavvio automatico consente all'uscita del DCS (O1) di eseguire il reset automatico in seguito ad una richiesta di intervento. L'azione manuale richiesta per garantire la sicurezza normalmente è indicata nel ramo 1 per il ripristino dell'abilitazione dell'uscita di sicurezza.

Input Status normalmente rappresenta lo stato di canale dei due canali d'ingresso. In questo esempio, il bit Combined Input Status passa a LO in caso di guasto su uno qualunque degli 8 canali d'ingresso.

In questo esempio il reset DCS funziona come un reset degli errori. Anche se si esegue la configurazione per il riavvio automatico, è sempre necessario eseguire un reset per il ripristino da un guasto/errore.

L'uscita (O1) dell'istruzione DCS è utilizzata come interblocco di sicurezza nel ramo seal-in (a ritenuta) per comandare il tag di abilitazione dell'uscita. Se l'uscita DCS viene diseccitata, lo stesso accade anche per l'abilitazione dell'uscita, che rimarrà disattivata fino a quando non verrà eseguita un'azione di reset manuale.

L'istruzione CROUT (Configurable Redundant Output) controlla e monitora le uscite ridondanti. Sostanzialmente, questa istruzione verifica che il feedback segua correttamente le uscite di sicurezza. Nel caso del feedback negativo utilizzato in questo esempio, se le uscite sono HI, il feedback deve essere LO, e viceversa. In questo esempio, il feedback ha 500 ms per passare allo stato corretto. Dal momento che viene utilizzato un solo circuito di feedback, il tag di feedback è utilizzato per i Feedback 1 e 2.

I due (2) tag di uscita dell'istruzione CROUT sono utilizzati per comandare le uscite dei contattori sul modulo 1734-OB8S.

Reset su fronte di discesa

Lo standard ISO 13849-1 stabilisce che le funzioni di reset delle istruzioni devono corrispondere ai fronti di discesa dei segnali. Per soddisfare questo requisito, aggiungere un'istruzione OSF (One Shot Falling) al ramo immediatamente precedente il ramo Cmd_Zone1_OutputEnable, quindi utilizzare il tag Output Bit dell'istruzione OSF come bit di reset per il ramo successivo. Cmd_Zone1_OutputEnable è ancora utilizzato per abilitare l'istruzione CROUT.

Il codice così modificato è visibile di seguito nei rami 1 e 2.

Calcolo dei livelli prestazionali

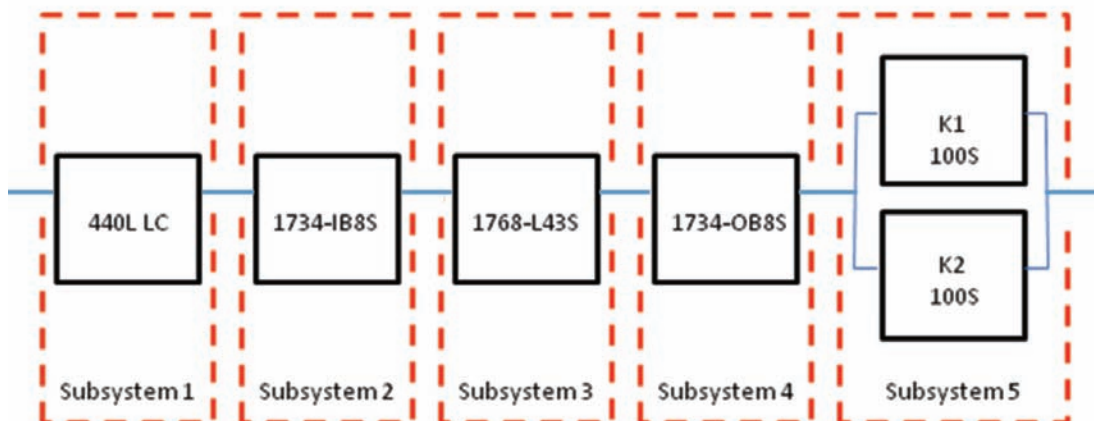
Se la configurazione è eseguita correttamente, la funzione di sicurezza di arresto di emergenza con barriera fotoelettrica può raggiungere un livello di sicurezza pari a PLe, CAT 4 secondo EN ISO 13849.1 2008.

Le specifiche di sicurezza funzionale del progetto richiedono un livello prestazionale pari a PLd (minimo) ed una struttura di Cat 3 (minimo). Il PLd prevede una probabilità di guasti pericolosi per ora (PFHd) inferiore a 1,0 E-06 per la funzione di sicurezza generale.

Di seguito sono riportati i valori dei singoli sottosistemi.

	Name	PL	PFH [1/h]	CCF score	DCavg [%]	MTTFd [a]	Category	Requirements of the category
SB	POINT Guard I/O: 1734-IB8S	e	1.34E-10	not relevant	not relevant	not relevant	4	fulfilled
SB	POINT Guard I/O: 1734-OB8S	e	1.38E-10	not relevant	not relevant	not relevant	4	fulfilled
SB	Safety PLC: Compact GuardLogix 1768	e	2.1E-10	not relevant	not relevant	not relevant	4	fulfilled
SB	Contactors 100S	e	2.47E-8	65 (fulfilled)	99 (High)	100 (High)	4	fulfilled
SB	Light Curtain: GuardShield 440L Type 4 - Single	e	3.17E-9	not relevant	not relevant	not relevant	4	fulfilled

Di seguito è riportato il valore generale della funzione di sicurezza.

La funzione di sicurezza LC può essere modellata come rappresentato nel seguente schema a blocchi di sicurezza:

I calcoli si basano su 1 intervento della barriera fotoelettrica all'ora, il che equivale a 8760 manovre dei contattori l'anno.

Le misure adottate contro i guasti per causa comune (Common Cause Failure – CCF) sono quantificate utilizzando il processo di classificazione descritto nell'Allegato F della norma ISO 13849-1. Ai fini del calcolo del livello prestazionale (PL), è necessario conseguire un livello di 65 per soddisfare il requisito relativo ai guasti CCF. Se si adotta questo esempio, occorre eseguire il processo completo di calcolo relativo ai guasti CCF.

SB Light Curtain: GuardShield 440L Type 4 - Single	
PL	e
PFH [1/h]	3.17E-9
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB POINT Guard I/O: 1734-IB8S	
PL	e
PFH [1/h]	1.34E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB Safety PLC: Compact GuardLogix 1768	
PL	e
PFH [1/h]	2.1E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB POINT Guard I/O: 1734-OB8S	
PL	e
PFH [1/h]	1.38E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

SB Contactors 100S	
PL	e
PFH [1/h]	2.47E-8
Cat.	4
MTTFd [a]	100 (High)
DCavg [%]	99 (High)
CCF	65 (fulfilled)

Piano di verifica e validazione

La verifica e la validazione hanno un ruolo importante, poiché contribuiscono ad evitare i guasti e gli errori in tutto il processo di progettazione e sviluppo del sistema di sicurezza. I requisiti per la verifica e la validazione sono definiti dalla norma ISO/EN 13849-2, che richiede la redazione di un piano documentato che comprovi l'effettivo rispetto di tutti i requisiti di sicurezza funzionale.

La verifica è l'analisi del sistema di controllo di sicurezza risultante. A questo scopo, si calcola il livello prestazionale (Performance Level – PL) del sistema di controllo di sicurezza, per verificare che sia conforme al livello prestazionale richiesto (Required Performance Level – PLr) specificato. Generalmente per eseguire i calcoli si utilizza lo strumento software SISTEMA, che aiuta l'utente a soddisfare i requisiti della ISO 13849-1.

La validazione è un collaudo funzionale del sistema di controllo di sicurezza, che serve a dimostrarne la rispondenza ai requisiti specificati della funzione di sicurezza. Il sistema di controllo di sicurezza viene collaudato per verificare che tutte le uscite di sicurezza rispondano correttamente agli ingressi di sicurezza corrispondenti. Il collaudo funzionale dovrebbe comprendere condizioni di funzionamento normali, oltre alle modalità di guasto basate sulla simulazione di potenziali guasti. Generalmente si utilizza una lista di controllo per documentare la validazione del sistema di controllo di sicurezza.

La validazione nel campo dello sviluppo software è un processo che prevede l'utilizzo di metodologie e tecniche simili a quelle utilizzate per lo sviluppo hardware. I guasti che si verificano a causa di processi e procedure di sviluppo software non ottimali sono di natura sistemica, a differenza dei guasti connessi all'hardware, che sono considerati di natura casuale.

Prima di eseguire la validazione del sistema di sicurezza GuardLogix, è necessario verificare che il sistema di sicurezza ed il programma applicativo di sicurezza siano stati progettati in conformità al Manuale di riferimento per la sicurezza Sistemi del controllore GuardLogix (1756-RM093) ed al Manuale di riferimento Set di istruzioni per l'applicazione di sicurezza GuardLogix (1756-RM095).

Checklist di verifica e validazione per funzione di sicurezza con barriera fotoelettrica GuardLogix

Informazioni generali sulla macchina	
Nome/numero di modello della macchina	
Numero di serie della macchina	
Nome del cliente	
Data di collaudo	
Nome/i dei collaudatori	
Numero di disegno	
Nome del controllore	
ID della firma di sicurezza	
Numero/i rete di sicurezza	
Versione del software RSLogix5000	

Moduli del sistema di controllo di sicurezza	Moduli GuardLogix	Versione del firmware
Controllore di sicurezza GuardLogix	1768-L43S	
Bridge Ethernet CompactLogix	1768-ENBT	
Scheda Ethernet POINT I/O	1734-AENT	
Moduli d'ingresso POINT I/O	1734-IB8S	
Moduli d'uscita POINT I/O	1734-OB8S	

Verifica di configurazione e cablaggio del sistema di sicurezza GuardLogix

Fase test	Verifica	Superato/non superato	Modifiche
1	Verificare che il sistema di sicurezza sia stato progettato in conformità al Manuale di riferimento per la sicurezza Sistemi del controllore GuardLogix 1756-RM093.		
2	Verificare che il programma applicativo di sicurezza sia stato progettato in conformità alle istruzioni d'applicazione per la sicurezza dei sistemi del controllore GuardLogix, Manuale di riferimento 1756-RM095.		
3	Ispezionare visivamente la rete del sistema di sicurezza e controllare che l'I/O sia cablato come indicato negli schemi.		
4	Verificare il programma RSLogix 5000 per controllare che la configurazione della rete del sistema di sicurezza e del modulo I/O sia conforme alla documentazione.		
5	Verificare il programma applicativo RSLogix 5000 per controllare che siano state utilizzate istruzioni di sicurezza certificate adatte. Verificare che la logica sia leggibile e comprensibile, e che possa essere testata con l'ausilio di commenti chiari.		
6	Verificare che tutti i dispositivi di ingresso siano funzionanti spegnendo e riaccendendo i rispettivi attuatori. Monitorare lo stato nella finestra Controller Tags di RSLogix 5000.		
7	Verificare che tutti i dispositivi di uscita siano funzionanti spegnendo e riaccendendo i rispettivi attuatori. Monitorare lo stato nella finestra Controller Tags di RSLogix 5000.		

Verifica di funzionamento normale – Il sistema di sicurezza GuardLogix deve rispondere correttamente a tutti i comandi normali di avviamento, arresto, abilitazione e reset

Fase test	Verifica	Superato/non superato	Modifiche
1	Inviare un comando di avviamento. I due contattori devono essere eccitati per determinare una condizione di normale funzionamento della macchina. Verificare che l'indicazione di stato della macchina e l'indicazione del programma applicativo di sicurezza RSLogix 5000 siano corrette.		
2	Inviare un comando di stop. I due contattori devono essere diseccitati per determinare una condizione di arresto normale della macchina. Verificare che l'indicazione di stato della macchina e l'indicazione del programma applicativo di sicurezza RSLogix 5000 siano corrette.		
3	Durante il normale funzionamento della macchina, interrompere la barriera fotoelettrica. I due contattori devono rimanere diseccitati ed aperti per determinare una condizione di sicurezza normale. Verificare che l'indicazione di stato della macchina e l'indicazione del programma applicativo di sicurezza RSLogix 5000 siano corrette.		
4	Con la macchina in condizione di arresto, interrompere la barriera fotoelettrica ed inviare un comando di avviamento. I due contattori devono rimanere diseccitati ed aperti per determinare una condizione di sicurezza normale. Verificare che l'indicazione di stato della macchina e l'indicazione del programma applicativo di sicurezza RSLogix 5000 siano corrette. Ripetere per tutte le barriere fotoelettriche.		
5	Inviare un comando di reset. I due contattori devono rimanere diseccitati. Verificare che l'indicazione di stato della macchina e l'indicazione del programma applicativo di sicurezza RSLogix 5000 siano corrette.		

Verifica di funzionamento anomalo – Il sistema di sicurezza GuardLogix deve rispondere correttamente a tutti i guasti prevedibili con le funzioni diagnostiche corrispondenti. Test relativi agli ingressi della barriera fotoelettrica			
Fase test	Validazione	Superato/non superato	Modifiche
1	Durante il normale funzionamento della macchina, staccare il cavo del canale 1 dall'I/O di sicurezza. I due contattori devono diseccitarsi. Verificare che l'indicazione di stato della macchina e l'indicazione del programma applicativo di sicurezza RSLogix 5000 siano corrette. Verificare che non sia possibile eseguire il reset e riavviare in presenza di guasto. Ripristinare il canale 1 e ripetere per il canale 2.		
2	Durante il normale funzionamento della macchina, cortocircuitare il canale 1 dell'I/O di sicurezza a +24 V CC. I due contattori devono diseccitarsi. Verificare che l'indicazione di stato della macchina e l'indicazione del programma applicativo di sicurezza RSLogix 5000 siano corrette. Verificare che non sia possibile eseguire il reset e riavviare in presenza di guasto. Ripristinare il canale 1 e ripetere per il canale 2.		
3	Durante il normale funzionamento della macchina, cortocircuitare il canale 1 dell'I/O di sicurezza a (–) 0 V CC. I due contattori devono diseccitarsi. Verificare che l'indicazione di stato della macchina e l'indicazione del programma applicativo di sicurezza RSLogix 5000 siano corrette. Verificare che non sia possibile eseguire il reset e riavviare in presenza di guasto. Ripristinare il canale 1 e ripetere per il canale 2.		
4	Durante il normale funzionamento della macchina, cortocircuitare i canali 1 e 2 dell'I/O di sicurezza. I due contattori devono diseccitarsi. Verificare che l'indicazione di stato della macchina e l'indicazione del programma applicativo di sicurezza RSLogix 5000 siano corrette. Verificare che non sia possibile eseguire il reset e riavviare in presenza di guasto. Ripristinare il cablaggio dei canali 1 e 2.		
Test per la rete ed il controllore GuardLogix			
Fase test	Validazione	Superato/non superato	Modifiche
1	Durante il normale funzionamento della macchina, disattivare la connessione di rete Ethernet tra l'I/O di sicurezza ed il controllore. Tutti i contattori devono diseccitarsi. Verificare che l'indicazione di stato della macchina e l'indicazione di stato della connessione di I/O nel programma applicativo di sicurezza RSLogix 5000 siano corrette.		
2	Ripristinare la connessione di rete del modulo I/O di sicurezza ed attendere un po' di tempo affinché la connessione venga riattivata. Verificare il bit di stato della connessione nel programma applicativo di sicurezza RSLogix 5000. Ripetere per tutte le connessioni di I/O di sicurezza.		
3	Durante il normale funzionamento della macchina, fare uscire il controllore dalla modalità Esecuzione. Tutti i contattori devono diseccitarsi. Riportare il selettore a chiave in modalità Esecuzione. Tutti i contattori devono rimanere diseccitati. Verificare che l'indicazione di stato della macchina e l'indicazione del programma applicativo di sicurezza RSLogix 5000 siano corrette.		
Test per le uscite dei contattori di sicurezza			
Fase test	Validazione	Superato/non superato	Modifiche
1	Inviare un comando di avviamento. I due contattori devono essere eccitati per determinare una condizione di normale funzionamento della macchina. Verificare che l'indicazione di stato della macchina e l'indicazione del programma applicativo di sicurezza RSLogix 5000 siano corrette.		
2	Durante il normale funzionamento della macchina, rimuovere il feedback del contattore dall'I/O di sicurezza. Tutti i contattori devono rimanere eccitati. Inviare un comando di stop e provare ad inviare un comando di reset. Il sistema non deve riavviarsi o resettarsi. Verificare che l'indicazione di stato della macchina e l'indicazione del programma applicativo di sicurezza RSLogix 5000 siano corrette.		
3	Durante il normale funzionamento della macchina, cortocircuitare il feedback del contattore all'I/O di sicurezza. Tutti i contattori devono rimanere eccitati. Inviare un comando di stop e provare ad inviare un comando di reset. Il sistema non deve riavviarsi o resettarsi. Verificare che l'indicazione di stato della macchina e l'indicazione del programma applicativo di sicurezza RSLogix 5000 siano corrette.		

Altre risorse

Per ulteriori informazioni sui prodotti utilizzati in questo esempio è possibile consultare la documentazione sotto indicata.

Risorsa	Descrizione
Manuale dell'utente Controllori Compact GuardLogix, pubblicazione 1768-UM002	Contiene informazioni sulla configurazione, il funzionamento e la manutenzione dei controllori Compact GuardLogix.
Manuale di installazione e uso Moduli di sicurezza POINT Guard I/O, pubblicazione 1734-UM013	Contiene informazioni sull'installazione, la configurazione e l'uso dei moduli POINT Guard I/O.
Manuale di riferimento per la sicurezza Sistemi di controllori GuardLogix, pubblicazione 1756-RM093	Contiene informazioni dettagliate sui requisiti per il conseguimento ed il mantenimento delle classi di sicurezza con il sistema di controllori GuardLogix.
Manuale di riferimento GuardLogix Safety Application Instruction Set, pubblicazione 1756-RM095	Contiene informazioni dettagliate sui set di istruzioni per l'applicazione di sicurezza GuardLogix.
Safety Accelerator Toolkit for GuardLogix Systems Quick Start Guide, pubblicazione IASIMP-QS005	Guida passo-passo all'uso degli strumenti di progettazione, programmazione e diagnostica del Safety Accelerator Toolkit.
Catalogo dei prodotti di sicurezza	

Per visualizzare o scaricare le pubblicazioni, visitare il sito http://www.rockwellautomation.com/literature. Per ordinare copie cartacee della documentazione tecnica, contattare il distributore Allen-Bradley® o il rappresentante Rockwell Automation di zona.

Per ulteriori informazioni sulle nostre soluzioni di sicurezza, visitare il sito

discover.rockwellautomation.com/safety

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americhe: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496, USA, Tel: +1 414 382 2000, Fax: +1 414 382 4444
Europa/Medio Oriente/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgio, Tel: +32 2 663 0600, Fax: +32 2 663 0640
Asia: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: +852 2887 4788, Fax: +852 2508 1846

Italia: Rockwell Automation S.r.l., Via Gallarate 215, 20151 Milano, Tel: +39 02 334471, Fax: +39 02 33447701, www.rockwellautomation.it
Svizzera: Rockwell Automation AG, Via Cantonale 27, 6928 Manno, Tel: 091 604 62 62, Fax: 091 604 62 64, Customer Service: Tel: 0848 000 279

Pubblicazione SAFETY-AT056B-IT-E – Gennaio 2013